

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

Nazwa zamówienia: Dostawa sprzętu informatycznego.

Numer referencyjny: ZF.272.1.8.2025

Załączniki do specyfikacji warunków zamówienia:

1. Szczegółowy opis przedmiotu zamówienia.
2. Widok interaktywnego formularza ofertowego.
3. Formularz rzeczowo – finansowy.
4. Oświadczenie o niepodleganiu wykluczeniu z postępowania.
5. Projektowane postanowienia umowy.

Rzeszów 10.04.2025

§ 1. Zamawiający

Powiat Rzeszowski
35-959 Rzeszów, ul. Grunwaldzka 15.

Postępowanie prowadzi:

Starostwo Powiatowe w Rzeszowie,
35-959 Rzeszów, ul. Grunwaldzka 15
telefon: 17 230 07 70;
e-mail: zampubliczne@powiat.rzeszowski.pl
dni i godziny pracy: poniedziałek - piątek, 7:30 – 15:30.

§ 2. Strona internetowa prowadzonego postępowania

1. Postępowanie prowadzone będzie przy użyciu **Platformy e-Zamówienia**, która jest dostępna pod adresem: <https://ezamowienia.gov.pl>.
2. Strona internetowa prowadzonego postępowania:
<https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-5bd7ae7c-09db-43fc-8b3f-aae0be1ef091>
Identyfikator postępowania na platformie e-Zamówienia:
ocds-148610-5bd7ae7c-09db-43fc-8b3f-aae0be1ef091
3. Zmiany i wyjaśnienia treści specyfikacji warunków zamówienia, zwanej dalej SWZ, oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem udostępniane będą na stronie internetowej prowadzonego postępowania wskazanej w ust. 2.

§ 3. Tryb udzielenia zamówienia

Zamówienie zostanie udzielone w trybie **podstawowym** zgodnie z **art. 275 pkt 1** ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2024 r. poz.1320 ze zm.), zwanej dalej ustawą pzp.

§ 4. Negocjacje

Najkorzystniejsza oferta zostanie wybrana bez przeprowadzenia negocjacji.

§ 5. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostawa i wdrożenie dwóch sprzętowych zapór sieciowych oraz systemu centralnego logowania, raportowania i korelacji wraz z niezbędnymi licencjami dla Starostwa Powiatowego w Rzeszowie.
Oznaczenie wg Wspólnego Słownika Zamówień (CPV):
32420000-3 urządzenia sieciowe,
48000000-8 pakiety oprogramowania i systemy informatyczne.
2. Zamawiający nie dopuszcza składania ofert częściowych. Dostawa sprzętu informatycznego jest zamówieniem podzielonym na części, z których każda stanowi przedmiot odrębnego postępowania, zaś aktualnie udzielane zamówienie jest jedną z części, której zakres obejmuje dostawę 2 sztuk sprzętowych zapór sieciowych oraz oprogramowania.
3. Miejsce dostawy: Starostwo Powiatowe w Rzeszowie, 35-959 Rzeszów, ul. Grunwaldzka 15.
4. Wymagania techniczne oraz warunki realizacji przedmiotu zamówienia zostały określone w załącznikach: „Szczegółowy opis przedmiotu zamówienia” oraz „Projektowane postanowienia umowy”.

§ 6. Termin wykonania zamówienia

Zamówienie należy zrealizować w terminie **do 30 dni** od dnia podpisania umowy.

§ 7. Warunki udziału w postępowaniu

Zamawiający nie określa warunków udziału w postępowaniu.

§ 8. Podmiotowe środki dowodowe

Zamawiający nie wymaga złożenia podmiotowych środków dowodowych.

§ 9. Wymagania dotyczące wadium

Zamawiający nie wymaga od wykonawców wniesienia wadium.

§ 10. Komunikacja z wykonawcami

1. Komunikacja w postępowaniu między zamawiającym a wykonawcą odbywa się za pośrednictwem Platformy e-Zamówienia, która dostępna jest pod adresem: <https://ezamowienia.gov.pl> oraz poczty elektronicznej.
2. Korzystanie z Platformy e-Zamówienia jest bezwzględnie wymagane dla przekazywania oferty oraz załączników do oferty.
3. Wykonawca zamierzający wziąć udział w postępowaniu, musi posiadać konto podmiotu „Wykonawca” na Platformie e-Zamówienia. Korzystanie z Platformy e-Zamówienia jest bezpłatne. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej <https://ezamowienia.gov.pl> oraz informacje zamieszczone w zakładce „Centrum Pomocy”.
4. Komunikacja w postępowaniu, z wyłączeniem składania ofert, odbywa się za pośrednictwem poczty elektronicznej (adres zamawiającego: zampubliczne@powiat.rzeszowski.pl) lub za pośrednictwem „Formularzy do komunikacji” dostępnych w zakładce „Formularze”. Za pośrednictwem poczty elektronicznej lub „Formularzy do komunikacji”, odbywa się w szczególności przekazywanie oświadczeń, wezwań, zawiadomień a także zadawanie pytań. Składanie ofert odbywa się za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania po zalogowaniu się na konto wykonawcy.
5. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji” wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
6. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia.
7. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu (22) 458 77 99 (czynny od poniedziałku do piątku w godzinach: 08:15-16:15) lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej <https://ezamowienia.gov.pl> w zakładce „Zgłoś problem”.
8. Jeżeli zamawiający lub wykonawca przekazują oświadczenia, wezwania oraz zawiadomienia lub zadają pytania za pośrednictwem poczty elektronicznej, każda ze stron na żądanie drugiej strony niezwłocznie potwierdza fakt ich otrzymania.
9. Osoby uprawnione do komunikowania się z wykonawcami:
Adam Janicki, Dorota Machej; e-mail: zampubliczne@powiat.rzeszowski.pl.
10. Interaktywna instrukcja obrazująca sposób komunikacji z wykorzystaniem Platformy e-Zamówienia dostępna jest na stronie internetowej <https://ezamowienia.gov.pl/pl/komponent-edukacyjny/w> zakładce „Komunikacja w postępowaniu”.

§ 11. Forma dokumentów i sposób podpisywania

1. Ofertę (formularz ofertowy i formularz rzeczowo - finansowy), oświadczenie, o którym mowa w art. 125 ust.1 ustawy pzp oraz pełnomocnictwo, należy sporządzić w formie elektronicznej lub postaci elektronicznej i podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
2. Dokumenty elektroniczne, o których mowa w ust.1 przekazuje się jako załączniki.
3. Informacje, oświadczenia lub dokumenty, inne niż wymienione w ust.1 przekazywane w postępowaniu, sporządza się w postaci elektronicznej i przekazuje się jako załącznik lub jako tekst wpisany bezpośrednio do wiadomości e-mail lub w treści „Formularza do komunikacji”.
4. Dokumenty elektroniczne powinny być sporządzone w formatach danych określonych w przepisach rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773). Rekomendowane formaty danych:
 - dla formularza ofertowego: .pdf,

- dla oświadczeń i dokumentów składanych wraz z ofertą: .pdf, .odt, .doc, .docx, .jpg,
 - dla plików poddanych kompresji: .zip lub .7Z.
5. Sposób sporządzenia i przekazywania dokumentów elektronicznych musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r. poz. 2452) w szczególności z uwzględnieniem poniższych zasad:
- 1) W przypadku gdy dokumenty potwierdzające umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego lub podwykonawcy, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania”, zostały wystawione przez upoważnione podmioty inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia lub podwykonawca, zwane dalej „upoważnionymi podmiotami”, jako dokument elektroniczny, przekazuje się ten dokument.
 - 2) W przypadku gdy dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej dokonuje odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia lub podwykonawca, w zakresie dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą.
 - 3) Pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
 - 4) W przypadku gdy pełnomocnictwo, zostało sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej dokonuje mocodawca.
 - 5) Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej może dokonać również notariusz.
 - 6) Przez cyfrowe odwzorowanie z dokumentem w postaci papierowej, należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.
6. **W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty, kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.**

§ 12. Opis sposobu przygotowania i składania oferty

1. Wykonawca może złożyć jedną ofertę.
2. Oferta musi być sporządzona pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej, i opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
3. Ofertę podpisuje osoba uprawniona do reprezentacji wykonawcy zgodnie z formą reprezentacji wykonawcy określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej lub upoważniony przedstawiciel wykonawcy.
4. Ofertę należy sporządzić w języku polskim wykorzystując interaktywny „Formularz ofertowy” udostępniony przez zamawiającego na Platformie e-Zamówienia i zamieszczony w podglądzie postępowania w zakładce „Informacje podstawowe”. Dokumenty sporządzone w języku obcym należy złożyć wraz z tłumaczeniem na język polski.
5. Zalogowany wykonawca używając przycisku „Wypełnij” widocznego pod „Formularzem ofertowym” zobowiązany jest do zweryfikowania poprawności danych automatycznie pobranych przez system

z jego konta i uzupełnienia pozostałych informacji dotyczących wykonawcy/wykonawców wspólnie ubiegających się o udzielenie zamówienia.

6. Następnie wykonawca powinien pobrać „Formularz ofertowy”, zapisać go na dysku swojego komputera, uzupełnić pozostałymi danymi wymaganymi przez zamawiającego i ponownie zapisać na dysku swojego komputera oraz podpisać odpowiednim rodzajem podpisu elektronicznego, zgodnie z ust. 10.

UWAGA: Nie należy zmieniać nazwy pliku nadanej przez Platformę e-Zamówienia. Zapisany „Formularz oferty” należy otwierać i edytować w programie Adobe Acrobat Reader.

7. Wykonawca składa ofertę za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania po zalogowaniu się na konto wykonawcy. Po wybraniu przycisku „Złóż ofertę” system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola „przeciągnij i upuść” służące do dodawania plików.
8. Wykonawca dodaje wybrany z dysku i uprzednio podpisany „Formularz ofertowy” w pierwszym polu „Wypełniony formularz ofertowy”. W kolejnym polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę” wykonawca dodaje pozostałe pliki stanowiące ofertę lub składane wraz z ofertą.
9. Jeżeli wraz z ofertą składane są dokumenty zawierające tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2022 r. poz.1233), wykonawca w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”. Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane jako bezskuteczne ze względu na zaniechanie przez wykonawcę podjęcia niezbędnych działań w celu utrzymania poufności objętych klauzulą informacji, zgodnie z postanowieniami art. 18 ust. 3 ustawy pzp. Zarówno załącznik stanowiący tajemnicę przedsiębiorstwa jak i uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa należy dodać w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.
10. „Formularz ofertowy” podpisuje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Rekomendowanym wariantem podpisu jest typ wewnętrzny. Podpis „Formularza ofertowego” wariantem podpisu w typie zewnętrznym również jest możliwy, ale wówczas powstały oddzielny plik podpisu dla tego formularza należy załączyć w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.

UWAGA:

W związku ze zmianami po stronie Profilu Zaufanego obecnie nie ma możliwości podpisywania „podpisem zaufanym” interaktywnego formularza ofertowego, tak jak do tej pory. Aby podpisać formularz ofertowy pobrany z Platformy e-Zamówienia należy po pobraniu i wypełnieniu formularza zapisać go w wersji nieedytowalnej i następnie podpisać „podpisem zaufanym”.

W razie problemów z podpisem zaufanym pomoc można uzyskać telefonując pod numer: (42) 253 54 50 (czynny od poniedziałku do piątku w godzinach: 7:00 – 18:00) lub pisząc na adres e-mail:

pz-pomoc@coi.gov.pl lub epuap-pomoc@coi.gov.pl .

W sprawach związanych z formularzem ofertowym pomoc można uzyskać kontaktując się z Infolinią Platformy e-Zamówienia pod numerem telefonu: (22) 458 77 99 (czynny od poniedziałku do piątku w godzinach: 08:15-16:15).

11. Pozostałe dokumenty wchodzące w skład oferty lub składane wraz z ofertą, podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być opatrzone podpisem typu zewnętrznego lub wewnętrznego.
12. Maksymalny łączny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250 MB.
13. Wykonawca może przed upływem terminu składania ofert wycofać ofertę. Wykonawca wycofuje ofertę w zakładce „Oferty/wnioski” używając przycisku „Wycofaj ofertę”.
14. Zamawiający nie przewiduje możliwości złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty.
15. Zamawiający nie dopuszcza składania ofert wariantowych.

16. Do oferty należy dołączyć:

- 1) **Formularz rzeczowo – finansowy** - wg wzoru stanowiącego załącznik do SWZ.
- 2) **Oświadczenie o niepodleganiu wykluczeniu z postępowania**, o którym mowa w art. 125 ust. 1 ustawy pzp - wg wzoru stanowiącego załącznik do SWZ, odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia.
- 3) **Odpis lub informację** z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, w celu potwierdzenia, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania.
Wykonawca nie jest zobowiązany do złożenia ww. dokumentów, jeżeli zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, **o ile wykonawca wskazał dane umożliwiające dostęp do tych dokumentów**.
- 4) **Pełnomocnictwo** lub inny dokument potwierdzający umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia - **w przypadku reprezentowania wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia przez pełnomocnika**. Pełnomocnictwo musi być złożone w oryginale w takiej samej formie, jak składana oferta. Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego zgodnie z art. 97 § 2 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie (Dz.U. z 2024 r. poz.1001), które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez pełnomocnika, któremu udzielono przedmiotowego pełnomocnictwa.

17. Interaktywna instrukcja obrazująca sposób składania oferty z wykorzystaniem Platformy e-Zamówienia dostępna jest na stronie internetowej <https://ezamowienia.gov.pl/pl/komponent-edukacyjny/wzakladce> „Oferty, wnioski i prace konkursowe”.

§ 12a. Oferta wspólna

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.
2. W przypadku, o którym mowa w ust. 1, wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
3. Przepisy dotyczące wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia.
4. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie, o którym mowa w art. 125 ust. 1 ustawy pzp, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia każdego z wykonawców oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
5. Jeżeli zostanie wybrana oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, zamawiający może zażądać przed zawarciem umowy w sprawie zamówienia publicznego przedłożenia kopii umowy regulującej współpracę tych wykonawców.

§ 13. Termin składania ofert

Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie **do 18.04.2025 r. do godz.10:00**.

§ 14. Termin otwarcia ofert

1. Otwarcie ofert nastąpi **18.04.2025 r. o godz.10:10**.
2. Otwarcie ofert nastąpi przy użyciu systemu **Platforma e-Zamówienia**, w przypadku awarii tego systemu, która spowoduje brak możliwości otwarcia ofert w terminie określonym w ust.1, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
4. Niezwłocznie po otwarciu ofert Zamawiający udostępni na stronie internetowej prowadzonego postępowania informacje, o których mowa w art. 222 ust. 5 ustawy pzp.

§ 15. Termin związania ofertą

Wykonawca jest związany ofertą do **16.05.2025 r.**

§ 16. Podstawy wykluczenia

1. Zamawiający, na podstawie art. 108 ust.1 ustawy pzp, wykluczy z postępowania, z zastrzeżeniem art. 110 ust.2 ustawy pzp, wykonawcę:
 - 1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
 - a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 2024 r. poz.17 ze zm.) zwanej dalej Kodeksem karnym,
 - b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
 - c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz.U. z 2024 r. poz.1488) lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2024 r. poz.930 ze zm.),
 - d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
 - e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
 - f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz.U. z 2021 r. poz.1745),
 - g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
 - h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej
- lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
 - 2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
 - 3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
 - 4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
 - 5) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2024 r. poz.594), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykazą, że przygotowali te oferty lub wnioski niezależnie od siebie;
 - 6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 ustawy pzp, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

2. Zamawiający, na podstawie art.109 ust.1 pkt 4 ustawy pzp, wykluczy z postępowania wykonawcę: w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.
3. Zamawiający, na podstawie art.7 ust.1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2024 r. poz.507 ze zm.), zwanej dalej ustawą sankcyjną, wykluczy z postępowania wykonawcę:
 - 1) wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy sankcyjnej;
 - 2) którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2023 r. poz.1124 ze zm.) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy sankcyjnej;
 - 3) którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2023 r. poz. 120 ze zm.), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy sankcyjnej.

§ 17. Sposób obliczenia ceny

1. W cenie wykonawca zobowiązany jest uwzględnić wszystkie składniki i koszty mające wpływ na jej wysokość uwzględniając informacje i wymogi zawarte w szczegółowym opisie przedmiotu zamówienia.
2. Cenę oferty należy podać w złotych polskich z dokładnością do dwóch miejsc po przecinku.
3. Wykonawca określa cenę za wykonanie zamówienia, poprzez wskazanie w „Formularzu ofertowym” (pkt.VIII. Kryteria oceny ofert) ceny brutto oferty, z uwzględnieniem kwoty podatku od towarów i usług VAT. Cenę należy obliczyć wypełniając „Formularz rzeczowo – finansowy”. Wypełniony „Formularz rzeczowo – finansowy” należy złożyć wraz z „Formularzem ofertowym”. W przypadku rozbieżności pomiędzy kwotą wskazaną w „Formularzu ofertowym” a kwotą wskazaną w „Formularzu rzeczowo – finansowym”, jako poprawna zostanie przyjęta kwota wynikająca z „Formularza rzeczowo – finansowego”.
4. Jeżeli wybór oferty prowadził będzie do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2024 r. poz.361 ze zm.), wykonawca ma obowiązek w ofercie: poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego; wskazania nazwy (rodzaju) towaru, którego dostawa będzie prowadziła do powstania obowiązku podatkowego; wskazania wartości towaru objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku; wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.
5. Wszelkie rozliczenia z zamawiającym będą odbywać się wyłącznie w złotych polskich.

§ 18. Opis kryteriów oceny ofert, wraz z podaniem wag tych kryteriów, i sposobu oceny ofert

1. Przy ocenie ofert i wyborze najkorzystniejszej oferty, zamawiający będzie się kierował kryterium ceny.
2. Za najkorzystniejszą zostanie uznana ta z ofert niepodlegających odrzuceniu, której cena będzie najniższa lub oferta, która będzie jedyną ofertą złożoną w postępowaniu niepodlegającą odrzuceniu.

§ 19. Projektowane postanowienia umowy

Projektowane postanowienia umowy określone zostały w załączniku „Projektowane postanowienia umowy”.

§ 20. Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

Zawarcie umowy nastąpi w trybie i terminie ustalonym między stronami.

§ 21. Informacje dotyczące zabezpieczenia należytego wykonania umowy

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

§ 22. Pouczenie o środkach ochrony prawnej przysługujących wykonawcy

1. Środki ochrony prawnej przysługują wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy pzp.
2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 ustawy pzp, oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Zasady wnoszenia środków ochrony prawnej określa Dział IX ustawy pzp (Art. 505 – 590) „Środki ochrony prawnej”.

§ 23. Informacje uzupełniające

1. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
2. Zamawiający nie przewiduje aukcji elektronicznej.

§ 24. Klauzula informacyjna

Na podstawie art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L z 2016 r. Nr 119, str. 1), dalej „RODO”, informuję, że:

- 1) Administratorem Pani/Pana danych osobowych jest Starostwo Powiatowe w Rzeszowie, ul. Grunwaldzka, 15, 35 – 959 Rzeszów, które realizuje zadania Starosty Rzeszowskiego oraz Zarządu Powiatu. Kontakt telefoniczny: 17 23 00 651, kontakt e-mail: starostwo@powiat.rzeszowski.pl.
- 2) W zakresie dotyczącym ochrony danych osobowych może Pani/Pan kontaktować się pisemnie z Inspektorem Ochrony Danych pod adresem: ul. Grunwaldzka 15, 35 – 959 Rzeszów, lub za pomocą adresu e-mail: rodo@powiat.rzeszowski.pl.
- 3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem;
- 4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy pzp;
- 5) Pani/Pana dane osobowe będą przechowywane, przez okres określony zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r. Nr 14 poz.67 ze zm.);
- 6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy pzp;
- 7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- 8) posiada Pani/Pan:
 - a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących,
 - b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (*Skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*),
 - c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (*Prawo do ograniczenia*

przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.),

d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

9) nie przysługuje Pani/Panu:

a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,

b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,

c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

A. Wymagania ogólne

Oferowane urządzenia i oprogramowanie muszą spełniać następujące warunki:

1. Wszystkie urządzenia i oprogramowanie muszą pochodzić z legalnego kanału dystrybucji producenta, a korzystanie przez zamawiającego z dostarczonych urządzeń i oprogramowania nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, nigdy wcześniej nie instalowane i aktywowane na innym urządzeniu.
3. Wykonawca zobowiązany jest dostarczyć klucze licencyjne lub dokumenty potwierdzające prawo do korzystania z dostarczonych licencji przez zamawiającego.
4. Wszystkie licencje muszą być przeznaczone do użytku na terenie Rzeczypospolitej Polskiej.
5. Wykonawca zobowiązany jest do przestrzegania ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2022 r. poz.2509).
6. Wszystkie urządzenia muszą być:
 - 1) fabrycznie nowe, nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu poprawnej pracy,
 - 2) wyprodukowane nie wcześniej niż w 2024 roku,
 - 3) dostarczone wraz z dokumentacją zawierającą: instrukcje obsługi, karty gwarancyjne (w przypadku gdy producent nie stosuje dokumentacji papierowej, wykonawca zobowiązany jest dostarczyć dokumentację w postaci elektronicznej lub wskazać adres strony internetowej do jej pobrania),
 - 4) oznakowane w taki sposób, aby możliwa była identyfikacja modelu i producenta oraz dostarczone w oryginalnym opakowaniu.
7. Wszystkie urządzenia muszą posiadać możliwość sprawdzenia legalności i konfiguracji po podaniu numeru seryjnego na stronie producenta lub poprzez dedykowane narzędzie do weryfikacji numerów seryjnych.
8. Wszystkie urządzenia oraz system centralnego logowania i analizy zdarzeń muszą posiadać certyfikat bezpieczeństwa EAL4+ lub równoważny w ramach normy Common Criteria.
9. Wszystkie urządzenia muszą posiadać oznakowanie CE zgodnie z wymogami określonymi w Rozporządzeniu Ministra Rozwoju z dnia 2 czerwca 2016 r. w sprawie wymagań dla sprzętu elektrycznego (Dz. U. z 2016 r. poz. 806).
10. Okres gwarancji: 60 miesięcy.

B. Wymagania szczegółowe i parametry techniczne urządzeń i oprogramowania

1. SPRZĘTOWA ZAPORA SIECIOWA – 2 SZT.

Minimalne wymagania techniczne dla zapory sieciowej

- 1.1. Urządzenie musi stanowić platformę sprzętową wyposażoną w zintegrowany system operacyjny.
- 1.2. Urządzenie musi być wyposażone w dwa wewnętrzne zasilacze 230V AC pracujące w trybie redundantnym.
- 1.3. Urządzenie musi mieć być przystosowane do montażu w szafie RACK 19", wysokość maksymalna 1U. Wraz z urządzeniem należy dostarczyć niezbędne elementy montażowe.
- 1.4. Urządzenie musi posiadać co najmniej następujące interfejsy:
 - 1) 10 portów Gigabit Ethernet RJ-45.
 - 2) 4 gniazd SFP 1 Gbps.
 - 3) 8 gniazd SFP+ 10 Gbps.
 - 4) wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
- 1.5. Urządzenie musi posiadać możliwość skonfigurowania co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- 1.6. Urządzenie musi posiadać konfigurację interfejsów redundantnych (failover), umożliwiających automatyczne przełączenie połączenia w przypadku awarii jednego z portów fizycznych.
- 1.7. Urządzenie musi posiadać agregację łączy w trybie statycznym oraz dynamicznym z wykorzystaniem protokołu LACP. Funkcja ta musi umożliwiać tworzenie logicznych interfejsów (LAG) z wielu portów fizycznych w celu zwiększenia przepustowości i zapewnienia redundancji połączenia.

- 1.8. Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (High Availability) w konfiguracji Active-Passive lub Active-Active, z funkcją synchronizacji sesji pomiędzy urządzeniami. Klaster musi zapewniać ciągłość działania i automatyczne przejęcie funkcji w przypadku awarii jednego z urządzeń.
- 1.9. Urządzenie musi posiadać co najmniej następujące parametry wydajnościowe:
 - 1) W zakresie Firewall'a obsługa nie mniej niż 11 mln jednoczesnych połączeń oraz 380 tys. nowych połączeń na sekundę.
 - 2) Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B.
 - 3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 25 Gbps.
 - 4) Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 34 Gbps.
 - 5) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 8 Gbps.
 - 6) Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps.
 - 7) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 7 Gbps.
- 1.10. Wymagania w zakresie funkcji systemu bezpieczeństwa:
 - 1) Kontrola dostępu - zaporę ogniową klasy Stateful Inspection.
 - 2) Kontrola Aplikacji.
 - 3) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
 - 4) Ochrona przed malware.
 - 5) Ochrona przed atakami - Intrusion Prevention System.
 - 6) Kontrola stron WWW.
 - 7) Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
 - 8) Zarządzanie pasmem (QoS, Traffic shaping).
 - 9) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
 - 10) Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.
 - 11) Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
 - 12) Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
 - 13) Wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
- 1.11. Wymagania w zakresie polityki firewall:
 - 1) Polityka Firewall uwzględniająca: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
 - 2) Możliwość realizacji translacji adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
 - 3) Możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
 - 4) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
 - 5) Polityka firewall umożliwiająca filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
 - 6) Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
 - 7) Element systemu realizujący funkcję Firewall musi integrować się co najmniej z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.

- VMware NSX.
- Kubernetes.

1.12. Wymagania w zakresie możliwości zestawienia połączeń VPN:

- 1) Możliwość konfiguracji połączeń typu IPsec VPN. W zakresie tej funkcji system musi zapewniać co najmniej :
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługę protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPsec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPsec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPsec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
- 2) Możliwość konfiguracji połączeń typu SSL VPN. W zakresie tej funkcji system musi zapewniać co najmniej: pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
- 3) Producent rozwiązania musi posiadać w ofercie darmowe oprogramowanie klienckie VPN umożliwiające realizację połączeń typu IPsec VPN oraz SSL VPN.

1.13. Wymagania w zakresie routingu i obsługi łącz WAN:

- 1) W zakresie routingu rozwiązanie musi zapewniać co najmniej:
 - Obsługę routingu statycznego.
 - Obsługę Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
 - Obsługę protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
 - Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
 - Obsługę ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
 - Obsługę BFD (Bidirectional Forwarding Detection).
 - Obsługę monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
- 2) W zakresie obsługi łącz WAN rozwiązanie musi posiadać funkcję SD-WAN, umożliwiającą wykorzystanie protokołów dynamicznego routingu przy konfiguracji mechanizmów równoważenia obciążenia pomiędzy łączami WAN

1.14. Wymagania w zakresie zarządzania pasmem:

- 1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- 2) System musi umożliwiać określanie pasma dla poszczególnych aplikacji.
- 3) System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
- 4) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

1.15. Wymagania w zakresie ochrony przed malware:

- 1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 21).
- 2) Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

- 3) W przypadku archiwów zagnieżdżonych możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub możliwość konfiguracji maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
- 4) System musi umożliwić blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
- 5) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
- 6) Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- 7) Urządzenie musi być zgodne z rozwiązaniami chmurowymi producenta, jednak logowanie i raportowanie musi być możliwe do realizacji w całości lokalnie – bez konieczności korzystania z usług chmurowych.
- 8) System musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
- 9) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
- 10) Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

1.16. Wymagania w zakresie ochrony przed atakami:

- 1) Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- 2) System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach.
- 3) Baza sygnatur ataków zawierająca minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- 4) Możliwość definiowania własnych wyjątków oraz własnych sygnatur przez administratora systemu.
- 5) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- 6) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
- 7) Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
- 8) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
- 9) Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

1.17. Wymagania w zakresie kontroli aplikacji:

- 1) Funkcja Kontroli Aplikacji umożliwiająca kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- 2) Baza Kontroli Aplikacji zawierająca minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- 3) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- 4) Baza sygnatur zawierająca kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- 5) Możliwość definiowania wyjątków oraz własnych sygnatur przez administratora systemu.
- 6) Możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
- 7) Możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

1.18. Wymagania w zakresie kontroli WWW:

- 1) Moduł kontroli WWW korzystający z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
- 2) W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
- 3) Filtr WWW dostarczający kategorii stron zabronionych prawem np.: Hazard.
- 4) Możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL przez administratora systemu.

- 5) Filtr WWW umożliwiający statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwalający definiować strony z zastosowaniem wyrażeń regularnych (Regex).
- 6) Filtr WWW umożliwiający wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
- 7) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
- 8) Możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW przez administratora systemu.
- 9) Możliwość określenia, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

1.19. Wymagania w zakresie uwierzytelniania użytkowników w ramach sesji:

- 1) Możliwość weryfikacji przez system tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
- 2) Możliwość zastosowania uwierzytelniania wieloskładnikowego.
- 3) Możliwość budowy architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
- 4) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

1.20. Wymagania w zakresie zarządzania:

- 1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
- 2) Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- 3) Możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
- 4) Systemem musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwić przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
- 5) Możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
- 6) Elementem systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- 7) Elementem systemu realizujący funkcję Firewall musi umożliwić wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
- 8) System musi umożliwiać przypisywanie administratorom uprawnień do zarządzania określonymi częściami systemu (RBM) oraz zdefiniowanie co najmniej 5 niezależnych administratorów, którym można przypisać osobne instancje lub obszary administracyjne systemu.
- 9) Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

1.21. Wymagania w zakresie logowania:

- 1) W ramach logowania element systemu pełniący funkcję Firewall musi zapewniać przekazywanie danych o:
 - a) zaakceptowanym ruchu,
 - b) blokowanym ruchu,
 - c) aktywności administratorów,
 - d) zużyciu zasobów oraz stanie pracy systemu.
 Ponadto musi zapewniać możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
- 2) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
- 3) Możliwość włączenia logowania per reguła w polityce firewall.
- 4) Możliwość logowania do serwera SYSLOG.
- 5) Możliwość przesyłania SYSLOG do zewnętrznych systemów z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

1.22. Wymagania w zakresie licencji i wsparcia technicznego:

- 1) Wraz z urządzeniami należy dostarczyć licencje, które muszą obejmować następujące funkcje: kontrola aplikacji; system IPS; antywirus (w tym sygnatury dla ochrony urządzeń mobilnych, co najmniej dla systemu Android); analiza typu Sandbox w modelu chmurowym; antyspam; filtrowanie stron WWW (Web Filtering); bazy reputacyjne adresów IP i domen.
Licencje muszą obejmować okres co najmniej 60 miesięcy. W przypadku dostarczenia urządzeń z licencjami bezterminowymi wykonawca wskazuje to w formularzu rzeczowo-finansowym. Jeżeli rodzaj licencji nie zostanie określony zamawiający przyjemnie, że obejmują one okres 60 miesięcy.
- 2) Urządzenia muszą być objęte bezpłatnym wsparciem technicznym producenta w okresie gwarancji.
- 3) Szczegółowe wymagania w zakresie gwarancji i wsparcia technicznego określone zostały w „projektowanych postanowieniach umowy”.

2. SYSTEM CENTRALNEGO LOGOWANIA I ANALIZY ZDARZEŃ – 1 SZT.

Minimalne wymagania techniczne dla systemu centralnego logowania i analizy zdarzeń

System do centralnego logowania, raportowania i korelacji, ma umożliwiać centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

System musi zostać dostarczony w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2016, 2019, 2025; Open Source Xen 4.1+, KVM.

Oferowany system musi:

- obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.
- być w stanie przyjmować minimum 5 GB logów na dzień.
- umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

1. Logowanie

W zakresie logowania system musi zapewniać:

- 1) Podgląd logowanych zdarzeń w czasie rzeczywistym.
- 2) Możliwość przeglądania logów historycznych z funkcją filtrowania.
- 3) System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa, muszą one obejmować co najmniej:
 - a) Listę najczęściej wykrywanych ataków.
 - b) Listę najbardziej aktywnych użytkowników.
 - c) Listę najczęściej wykorzystywanych aplikacji.
 - d) Listę najczęściej odwiedzanych stron www.
 - e) Listę krajów, do których nawiązywane są połączenia.
 - f) Listę najczęściej wykorzystywanych polityk Firewall.
 - g) Informacje o realizowanych połączeniach IPSec.
- 4) Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
- 5) Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
- 6) System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

2. Raportowanie

W zakresie raportowania system musi zapewniać:

- 1) Generowanie raportów co najmniej w formatach: PDF, CSV.
- 2) Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
- 3) Funkcję definiowania własnych raportów.
- 4) Możliwość spolszczenia raportów.

- 5) Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

3. Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

- 1) Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
- 2) Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
- 3) Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
 - a) Malware.
 - b) Aplikacje sieciowe.
 - c) Email.
 - d) IPS.
 - e) Traffic.
 - f) Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

4. Zarządzanie

W zakresie zarządzania system musi zapewniać:

- 1) Możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
- 2) Aby proces uwierzytelniania administratorów realizowany był w oparciu o: lokalną bazę, Radius, LDAP, PKI.
- 3) Możliwość zdefiniowania co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

5. Wymagania w zakresie licencji i wsparcia technicznego

- 1) System musi być dostarczony z licencją bezterminową w modelu „na własność” rozumianym w ten sposób, że: niewykupienie odnowienia wsparcia technicznego dla systemu nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
- 2) System musi być objęty bezpłatnym wsparciem technicznym producenta przez okres 60 miesięcy.
- 3) Szczegółowe wymagania w zakresie gwarancji i wsparcia technicznego określone zostały w „projektowanych postanowieniach umowy”.

C. Wdrożenie dostarczonych urządzeń i oprogramowania

W ramach realizacji zamówienia Wykonawca zobowiązany jest do wdrożenia dostarczonych zapór sieciowych oraz systemu centralnego logowania, raportowania i korelacji oraz przeprowadzenia 2-dniowego szkolenia praktycznego, w ilości minimum 4 h każdego dnia, dla pracowników zamawiającego w zakresie obsługi zamontowanych urządzeń.

1. Wymagania w zakresie wdrożenia zapór sieciowych.

- 1) Wykonawca przeprowadzi montaż zapór sieciowych obejmujący:
 - a) fizyczną instalację dwóch urządzeń w szafie RACK oraz podłączenie do infrastruktury sieciowej Zamawiającego,
 - b) podłączenie urządzeń do zasilania, w tym zapewnienie redundancji poprzez podłączenie do dwóch niezależnych źródeł zasilania,
 - c) połączenie urządzeń w tryb wysokiej dostępności (HA) – Active-Passive lub Active-Active,
 - d) podłączenie interfejsów sieciowych do przełączników warstwy dostępowej oraz szkieletowej,
 - e) oznaczenie i udokumentowanie połączeń kablowych dla ułatwienia późniejszej konserwacji.
- 2) Wykonawca skonfiguruje zapory sieciowe w następującym zakresie:
 - a) przeprowadzi aktualizację systemów operacyjnych do najnowszej stabilnej wersji rekomendowanej przez producenta,
 - b) skonfiguruje parametry urządzenia: adresacja IP, maska, brama domyślna,
 - c) przeprowadzi implementację polityk NAT i translacji adresów (SNAT, DNAT, PAT),
 - d) stworzy i przypisze interfejsy sieciowe do odpowiednich stref bezpieczeństwa (LAN, DMZ, WAN),

- e) skonfiguruje mechanizmy zabezpieczeń:
 - firewalla – reguły dostępu na podstawie źródła, celu, aplikacji, protokołów i czasu,
 - systemu zapobiegania włamaniom (IPS) – inspekcja pakietów i ochrona przed exploitami,
 - antywirusa i ochrona przed malware – skanowanie ruchu w czasie rzeczywistym,
 - kontroli aplikacji – blokowanie i zezwalanie na wybrane aplikacje w sieci,
 - inspekcji szyfrowanego ruchu SSL/TLS – filtrowanie niebezpiecznych zasobów online,
 - ochrony przed atakami DoS i DDoS,
 - zintegruje z listami reputacyjnymi (bazy zagrożeń, nask, reputacja adresów IP i domen),
 - f) skonfiguruje routing:
 - dynamiczny routing OSPF, BGP, RIP (jeśli wymagane),
 - routing statyczny dla połączeń wewnętrznych i zewnętrznych,
 - mechanizmy redundancji połączeń WAN i Load Balancing,
 - g) zaimplementuje mechanizmy zarządzania pasmem,
 - h) skonfiguruje filtrowanie ruchu sieciowego zgodnie z wymaganiami zamawiającego.
- 3) Wykonawca skonfiguruje VLAN i przeprowadzi segmentację sieci LAN zgodnie z zaleceniami lokalnego Informatyka w następującym zakresie:
- a) stworzy i przypisze VLAN do interfejsów,
 - b) skonfiguruje trunk i tagowanie ruchu,
 - c) wdroży polityki izolacji między VLAN-ami dla zwiększenia bezpieczeństwa,
 - d) zastosuje dynamiczny routingu między VLAN-ami.
- 4) Wykonawca skonfiguruje VPN-y w następującym zakresie:
- a) skonfiguruje tunele IPsec VPN Site-to-Site między lokalizacjami zamawiającego,
 - b) zaimplementuje SSL VPN dla użytkowników zdalnych:
 - uruchomi wsparcie dla różnych metod uwierzytelniania (LDAP, RADIUS, MFA),
 - skonfiguruje tryb split-tunneling dla optymalizacji ruchu,
 - uruchomi monitorowanie aktywności użytkowników VPN,
 - c) uruchomi automatyczne przełączanie tuneli VPN w przypadku awarii (Failover Mechanism),
 - d) przeprowadzi testy połączeń VPN oraz zweryfikuje logi sesji użytkowników.
- 5) Wykonawca przeprowadzi integrację z systemem analizy logów w następującym zakresie:
- a) zainstaluje i skonfiguruje oprogramowanie do centralnej analizy logów,
 - b) skonfiguruje logowanie zdarzeń związanych z:
 - sesjami użytkowników,
 - ruchem VPN,
 - zagrożeniami wykrywanymi przez IPS,
 - blokowanymi próbami dostępu i exploitami,
 - c) skonfiguruje tworzenie automatycznych alertów o wykrytych anomaliach sieciowych,
 - d) skonfiguruje retencję logów,
 - e) skonfiguruje generowanie raportów i powiadomień dla administratorów.
- 6) Wykonawca przeprowadzi testy funkcjonalne i obciążeniowe w następującym zakresie:
- a) wykona weryfikację poprawności polityk firewall oraz routingu,
 - b) przeprowadzi testy redundancji HA – wymuszone przełączenie aktywnego urządzenia,
 - c) zasymuluje próby włamań, ataków DDoS i innych zagrożeń,
 - d) przetestuje dostęp do zasobów przez użytkowników VPN,
 - e) przeprowadzi monitoring wydajności urządzenia pod obciążeniem.
- 7) Wykonawca opracuje oraz przekaże podczas odbioru przedmiotu umowy dokumentację powdrożeniową zawierającą:
- a) szczegółowy opis konfiguracji zapór,
 - b) procedury przywracania systemu i odzyskiwania danych.

2. Wymagania w zakresie wdrożenia systemu centralnego logowania i analizy zdarzeń.

- 1) Wykonawca w zakresie instalacji i konfiguracji systemu:
 - a) przeprowadzi instalację tak aby wdrożony system logowania był integralną częścią dostarczonej zapory sieciowej,

- b) zainstaluje system centralnego logowania w środowisku wirtualnym lub fizycznym zgodnie z wymaganiami zamawiającego,
 - c) zweryfikuje zgodności z dostępnymi hypervisorami (VMware ESX/ESXi, Microsoft Hyper-V),
 - d) przeprowadzi przygotowanie minimalnych zasobów systemowych, w tym interfejsy sieciowe i przestrzeń dyskową,
 - e) skonfiguruje ustawienia systemu, w tym integracji z siecią zamawiającego.
- 2) Wykonawca w zakresie konfiguracji zbierania i przechowywania logów:
- a) zdefiniuje polityki zbierania logów z zapory sieciowej oraz innych urządzeń sieciowych, serwerów, systemów operacyjnych i aplikacji,
 - b) przeprowadzi konfigurację komunikacji między systemami zabezpieczeń a centralnym systemem logowania przy użyciu protokołów UDP/514 oraz TCP/514,
 - c) wdroży mechanizmu długoterminowego przechowywania na zasobach sieciowych (SFTP, CIFS, NFS),
 - d) zweryfikuje poprawność zbierania logów i filtrowanie nieistotnych danych.
- 3) Wykonawca przeprowadzi konfigurację analizy logów i korelacji zdarzeń w ramach której:
- a) zdefiniuje reguły korelacji zdarzeń dla:
 - malware,
 - aplikacji sieciowych,
 - wiadomości e-mail,
 - systemu zapobiegania włamaniom (IPS),
 - ruchu sieciowego (Traffic),
 - utraconych połączeń VPN i awarii sieciowych,
 - b) skonfiguruje mechanizm alertowania w przypadku wykrycia zagrożeń (powiadomienia e-mail, SNMP),
 - c) przeprowadzi testy skuteczności korelacji i monitorowania incydentów.
- 4) Wykonawca w zakresie raportowania i monitoringu:
- a) dokona konfiguracji predefiniowanych raportów, obejmujących:
 - najczęściej wykrywanych ataków,
 - aktywność użytkowników,
 - używanych aplikacji,
 - odwiedzanych strony WWW,
 - statystyki połączeń VPN i polityk firewall.
 - b) skonfiguruje możliwość generowania raportów na żądanie lub cyklicznie w formatach PDF i CSV,
 - c) przeprowadzi testy automatycznego przesyłania raportów na wskazane adresy e-mail.
- 5) Wykonawca w zakresie zarządzania i uwierzytelnianie administratorów:
- a) dokona konfiguracji dostępu administracyjnego przez protokoły HTTPS i SSH,
 - b) dokona integracji z systemami uwierzytelniania (LDAP, Radius, PKI),
 - c) zdefiniuje co najmniej 4 administratorów z możliwością zarządzania uprawnieniami
 - d) skonfiguruje polityki dostępu do poszczególnych logów i raportów.
- 6) Wykonawca w zakresie testów funkcjonalnych i obciążeniowych:
- a) wykona testy poprawności zbierania i analizy logów,
 - b) przeprowadzi symulację incydentów i testowanie skuteczności wykrywania zagrożeń,
 - c) dokona weryfikacji poprawności integracji z urządzeniami i systemami monitorowania,
 - d) przeprowadzi testy wydajnościowe i optymalizacja zasobów systemowych.
- 7) Wykonawca opracuje oraz przekaze podczas odbioru przedmiotu umowy dokumentację powdrożeniową z zakresu:
- a) Szczegółowego opisu konfiguracji systemu logowania.
 - b) Instrukcji zarządzania politykami logowania i analizy zdarzeń.
 - c) Procedury odzyskiwania i przywracania systemu po awarii.
 - d) Dokumentacji integracji z innymi systemami monitorowania.

3. Wymagania w zakresie szkolenia.

- 1) Wykonawca przeprowadzi 2-dniowe szkolenie praktycznego, w ilości minimum 4 h każdego dnia, dla pracowników zamawiającego w zakresie obsługi wdrożonych urządzeń i oprogramowania.

- 2) Szkolenie przeprowadzone zostanie w siedzibie zamawiającego, w języku polskim, i obejmować będzie zagadnienia teoretyczne oraz warsztaty praktyczne.
- 3) Zagadnienia teoretyczne obejmować będą:
 - a) podstawy działania zapory sieciowej,
 - b) omówienie architektury wdrożonego systemu w tym systemu logowania,
 - c) omówienie podstawowych zasad analizy logów i korelacji zdarzeń,
 - d) funkcjonalność systemu analizy logów,
 - e) przedstawienie integracji systemu logowania z innymi platformami monitoringu,
 - f) obsługę interfejsu zarządzania,
 - g) tworzenie polityk dostępu i zabezpieczeń,
 - h) analiza logów, incydentów i tworzenie reguł korelacyjnych,
 - i) tworzenie raportów i alertów.
- 4) W ramach warsztatów praktycznych wykonawca przeprowadzi scenariusze awaryjne i procedurę odzyskiwanie systemu obejmujące:
 - a) reakcje na ataki i incydenty,
 - b) odzyskiwanie konfiguracji i testy HA.
- 5) Po zakończonym szkoleniu wykonawca prześle materiały dla uczestników na które składać się będą:
 - a) Podręcznik administratora.
 - b) Instrukcje szybkiej reakcji na incydenty.
 - c) Lista komend i skrótów do zarządzania systemem.
 - d) Certyfikaty potwierdzające udział w szkoleniu.

Widok interaktywnego formularza ofertowego.

UWAGA: Formularza nie należy wypełniać stanowi on jedynie obraz formularza udostępnionego na Platformie e-Zamówienia.

Dane identyfikacyjne formularza ofertowego

Numer wersji formularza ofertowego: 1

Data udostępnienia formularza ofertowego:

I. Dane podstawowe

Nazwa zamówienia/umowy ramowej: Dostawa sprzętu informatycznego.

Identyfikator postępowania: ocds-148610-5bd7ae7c-09db-43fc-8b3f-aae0be1ef091

Numer referencyjny postępowania: ZF.272.1.8.2025

Rodzaj oferty: Oferta

II. Zamawiający

Nazwa (firma) zamawiającego: POWIAT RZESZOWSKI

Krajowy numer identyfikacyjny: REGON 690581413

II.1 Zamawiający Adres

Ulica: ul. Grunwaldzka 15

Miejscowość: Rzeszów

Kod pocztowy: 35-959

Województwo: Podkarpackie

Kraj: Polska

III. Wykonawca

Nazwa (firma) wykonawcy:

Krajowy numer identyfikacyjny:

Status Wykonawcy:

III.1 Wykonawca Adres

Ulica:

Miejscowość:

Kod pocztowy:

Województwo:

Kraj:

Telefon:

Faks:

Adres poczty elektronicznej:

Adres strony internetowej
wykonawcy:

III.2 Wykonawca dane osoby reprezentującej

Czy wykonawca jest reprezentowany przez pełnomocnika: ☒ TAK ☐ NIE

Dane osoby reprezentującej (imię i nazwisko, podstawa reprezentacji - pełnomocnictwo, KRS, umowa spółki, inne):

III.3 Wykonawca Osoba do kontaktu

Dane osoby do kontaktu (imię i nazwisko, email, telefon):

IV. Oświadczenia

Wykonawca załącza do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy: ☒ TAK ☐ NIE

Adresy bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz. U. z 2020 r. poz. 346 z późn. zm.), gdzie można uzyskać oświadczenia lub inne dokumenty dotyczące wykonawcy:

<https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/index.html> ☒ TAK ☐ NIE

Rodzaje dokumentów dostępne pod wskazanym adresem:

<https://prod.ceidg.gov.pl/CEIDG/CEIDG.Public.UI/Se arch.aspx>

☒ TAK ☐ NIE

Rodzaje dokumentów dostępne pod wskazanym adresem:

Inne bazy

☒ TAK ☐ NIE

Adres:

Rodzaje dokumentów dostępne pod wskazanym adresem:

Dokumenty i oświadczenia znajdujące się w posiadaniu zamawiającego (rodzaj dokumentu, nazwa i numer postępowania, w którym zostały złożone):

Oświadczenie wykonawcy o spełnieniu obowiązku informacyjnego z art. 13 lub 14 Rozporządzenia Parlamentu Europejskiego i Rady 2016/679. (Klauzula RODO):

☒ TAK ☐ NIE

Treść oświadczenia*:

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

Wykonawca załącza do oferty oświadczenie o braku podstaw wykluczenia: TAK

V. Zamówienie zastrzeżone

Nie dotyczy

VI. Tajemnica przedsiębiorstwa

Oferta zawiera tajemnicę przedsiębiorstwa: ☒ TAK ☐ NIE

Informacje stanowiące tajemnicę przedsiębiorstwa zawarte są w następujących dokumentach (załącznikach do oferty):

Uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa zawarte jest w następującym dokumencie (załączniku do oferty):

VII. Katalog elektroniczny

Wykonawca załącza do oferty katalog elektroniczny: ☒ TAK ☐ NIE

VIII. Kryteria oceny ofert

Kod waluty: PLN

Rodzaj kryterium: Cena

Cena:

Wartość słownie:

IX. Obowiązek podatkowy

Wybór ofert będzie prowadził do powstania u zamawiającego obowiązku podatkowego: ☒ TAK ☐ NIE

Nazwa i wartość towaru lub usługi, której dostawa lub świadczenie będzie prowadzić do powstania obowiązku podatkowego:

X. Sposób realizacji zamówienia

Wykonawca zamierza powierzyć wykonanie części zamówienia podwykonawcy: ☒ TAK ☐ NIE

Nazwa podwykonawcy, jeżeli jest znany:

Zakres zamówienia, który wykonawca zamierza
powierzyć do realizacji podwykonawcy:

XII. Lista załączników

Lista
załączników:

Wzór dokumentu, nie wypełniać

Formularz rzeczowo – finansowy

Lp.	Określenie urządzenia/oprogramowania	Ilość	Stawka podatku VAT (%)	Wartość brutto (zł)
1	SPRZĘTOWA ZAPORA SIECIOWA PRODUCENT, NAZWA : Numer produktu lub kod producenta: Z urządzeniami zostaną dostarczone licencje: bezterminowe/terminowe na okres 60 miesięcy* OKRES GWARANCJI: 60 miesięcy.	2 szt.	23	
2	SYSTEM CENTRALNEGO LOGOWANIA I ANALIZY ZDARZEŃ PRODUCENT, NAZWA : Numer produktu lub kod producenta: LICENCJA: bezterminowa z bezpłatnym wsparciem technicznym na okres: 60 miesięcy.	1 szt.	23	
RAZEM WARTOŚĆ BRUTTO				

*-niepotrzebne skreślić lub usunąć

Oświadczam, że wszystkie oferowane urządzenia i oprogramowanie są zgodne z wymaganiami funkcjonalnymi i technicznymi określonymi w szczegółowym opisie przedmiotu zamówienia, a także posiadają parametry techniczne, nie gorsze niż parametry określone w szczegółowym opisie przedmiotu zamówienia.

WYKONAWCA

.....

.....

(nazwa, adres)

OŚWIADCZENIE

o niepodleganiu wykluczeniu z postępowania

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych,
zwanej dalej „ustawą pzp” w postępowaniu o udzielenie zamówienia publicznego,
pn.: **Dostawa sprzętu informatycznego.**

W zakresie przesłanek wykluczenia z postępowania

- 1) Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art.108 ust.1 a także art.109 ust.1 pkt 4 ustawy pzp.
- 2) Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust.1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2024 r. poz.507 ze zm.).
- 3) Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ustawy pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art.108 ust.1 pkt 1,2,5 lub art.109 ust.1 pkt 4 ustawy pzp).
Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art.110 ust. 2 ustawy pzp podjąłem następujące środki naprawcze:

.....
.....

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

Projektowane postanowienia umowy

Umowa nr ZF.272.1.8.2025

zawarta w dniu /zawarta w dniu złożenia ostatniego kwalifikowanego podpisu elektronicznego w Rzeszowie pomiędzy:

Powiatem Rzeszowskim z siedzibą w Rzeszowie przy ul. Grunwaldzkiej 15, 35-959 Rzeszów, REGON: 690581413, NIP: 8132919572, który reprezentują:

.....

.....

zwanym dalej w treści umowy **Zamawiającym**

a

.....

zwanym/zwaną dalej w treści umowy **Wykonawcą**

łącznie zwanymi dalej Stronami.

W wyniku przeprowadzenia postępowania o udzielenie zamówienia publicznego w trybie podstawowym zgodnie z art. 275 pkt.1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320), zwanej dalej ustawą pzp, strony zawarły umowę następującej treści:

PRZEDMIOT UMOWY

§1

1. Przedmiotem umowy jest dostawa i wdrożenie dwóch sprzętowych zapór sieciowych oraz systemu centralnego logowania, raportowania i korelacji wraz z niezbędnymi licencjami dla Starostwa Powiatowego w Rzeszowie.
2. Zapory sieciowe, zwane dalej urządzeniami, oraz oprogramowanie, o których mowa w ust. 1 wymienione są w „Wykazie rzeczowo-finansowym” stanowiącym załącznik do umowy.
3. Wszystkie urządzenia i oprogramowanie muszą pochodzić z legalnego kanału dystrybucji producenta, a korzystanie przez Zamawiającego z dostarczonych urządzeń i oprogramowania nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
4. Dostarczone oprogramowanie musi być fabrycznie nowe, nigdy wcześniej nie instalowane i aktywowane na innym urządzeniu.
5. Wykonawca zobowiązany jest dostarczyć klucze licencyjne lub dokumenty potwierdzające prawo do korzystania z dostarczonych licencji przez zamawiającego.
6. Wszystkie licencje muszą być przeznaczone do użytku na terenie Rzeczypospolitej Polskiej.
7. Wykonawca zobowiązany jest do przestrzegania ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2022 r. poz. 2509).
8. Wszystkie urządzenia muszą być:
 - 1) fabrycznie nowe, nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu poprawnej pracy,
 - 2) wyprodukowane nie wcześniej niż w 2024 roku,
 - 3) dostarczone wraz z dokumentacją zawierającą: instrukcje obsługi, karty gwarancyjne (w przypadku gdy producent nie stosuje dokumentacji papierowej, wykonawca zobowiązany jest dostarczyć dokumentację w postaci elektronicznej lub wskazać adres strony internetowej do jej pobrania),
 - 4) oznakowane w taki sposób, aby możliwa była identyfikacja modelu i producenta oraz dostarczone w oryginalnym opakowaniu.
9. Wszystkie urządzenia muszą posiadać możliwość sprawdzenia konfiguracji po podaniu numeru seryjnego na stronie producenta.
10. Wszystkie urządzenia muszą posiadać oznakowanie CE zgodnie z wymogami określonymi w Rozporządzeniu Ministra Rozwoju z dnia 2 czerwca 2016 r. w sprawie wymagań dla sprzętu elektrycznego (Dz. U. z 2016 r. poz. 806).

REALIZACJA UMOWY

§2

1. Przedmiot umowy zostanie wykonany w terminie **do 30 dni** od dnia zawarcia umowy.
2. Miejsce dostawy urządzeń: Starostwo Powiatowe w Rzeszowie, ul. Grunwaldzka 15, 35-959 Rzeszów.
3. Wykonawca zgłosi Zamawiającemu termin planowanej dostawy z co najmniej jednodniowym wyprzedzeniem.
4. W ramach realizacji umowy Wykonawca zobowiązany jest do wdrożenia dostarczonych zapór sieciowych oraz systemu centralnego logowania, raportowania i korelacji oraz przeprowadzenia 2-dniowego szkolenia praktycznego, w ilości minimum 4 h każdego dnia, dla pracowników zamawiającego w zakresie obsługi wdrożonych urządzeń i oprogramowania.
5. W ramach wdrożenia zapór sieciowych Wykonawca wykona poniższe czynności:
 - 1) przeprowadzi montaż zapór sieciowych obejmujący:
 - a) fizyczną instalację dwóch urządzeń w szafie RACK oraz podłączenie do infrastruktury sieciowej Zamawiającego,
 - b) podłączenie urządzeń do zasilania, w tym zapewnienie redundancji poprzez podłączenie do dwóch niezależnych źródeł zasilania,
 - c) połączenie urządzeń w tryb wysokiej dostępności (HA) – Active-Passive lub Active-Active,
 - d) podłączenie interfejsów sieciowych do przełączników warstwy dostępowej oraz szkieletowej,
 - e) oznaczenie i udokumentowanie połączeń kablowych dla ułatwienia późniejszej konserwacji,
 - 2) skonfiguruje zapory sieciowe w następującym zakresie:
 - a) przeprowadzi aktualizację systemów operacyjnych do najnowszej stabilnej wersji rekomendowanej przez producenta,
 - b) skonfiguruje parametry urządzenia: adresacja IP, maska, brama domyślna,
 - c) przeprowadzi implementację polityk NAT i translacji adresów (SNAT, DNAT, PAT),
 - d) stworzy i przypisze interfejsy sieciowe do odpowiednich stref bezpieczeństwa (LAN, DMZ, WAN),
 - e) skonfiguruje mechanizmy zabezpieczeń:
 - firewalla – reguły dostępu na podstawie źródła, celu, aplikacji, protokołów i czasu,
 - systemu zapobiegania włamaniom (IPS) – inspekcja pakietów i ochrona przed exploitami,
 - antywirusa i ochrona przed malware – skanowanie ruchu w czasie rzeczywistym,
 - kontroli aplikacji – blokowanie i zezwalanie na wybrane aplikacje w sieci,
 - inspekcji szyfrowanego ruchu SSL/TLS – filtrowanie niebezpiecznych zasobów online,
 - ochrony przed atakami DoS i DDoS,
 - zintegruje z listami reputacyjnymi (bazy zagrożeń, nask, reputacja adresów IP i domen),
 - f) skonfiguruje routing:
 - dynamiczny routing OSPF, BGP, RIP (jeśli wymagane),
 - routing statyczny dla połączeń wewnętrznych i zewnętrznych,
 - mechanizmy redundancji połączeń WAN i Load Balancing,
 - g) zaimplementuje mechanizmy zarządzania pasmem,
 - h) skonfiguruje filtrowanie ruchu sieciowego zgodnie z wymaganiami zamawiającego,
 - 3) skonfiguruje VLAN i przeprowadzi segmentację sieci LAN zgodnie z zaleceniami lokalnego Informatyka w następującym zakresie:
 - a) stworzy i przypisze VLAN do interfejsów,
 - b) skonfiguruje trunk i tagowanie ruchu,
 - c) wdroży polityki izolacji między VLAN-ami dla zwiększenia bezpieczeństwa,
 - d) zastosuje dynamiczny routingu między VLAN-ami.
 - 4) skonfiguruje VPN-y w następującym zakresie:
 - a) skonfiguruje tunele IPsec VPN Site-to-Site między lokalizacjami zamawiającego,
 - b) zaimplementuje SSL VPN dla użytkowników zdalnych:
 - uruchomi wsparcie dla różnych metod uwierzytelniania (LDAP, RADIUS, MFA).
 - skonfiguruje tryb split-tunneling dla optymalizacji ruchu,
 - uruchomi monitorowanie aktywności użytkowników VPN,
 - c) uruchomi automatyczne przełączanie tuneli VPN w przypadku awarii (Failover Mechanism),
 - d) przeprowadzi testy połączeń VPN oraz zweryfikuje logi sesji użytkowników.
 - 5) przeprowadzi integrację z systemem analizy logów w następującym zakresie:

- a) zainstaluje i skonfiguruje oprogramowanie do centralnej analizy logów,
 - b) skonfiguruje logowanie zdarzeń związanych z:
 - sesjami użytkowników,
 - ruchem VPN,
 - zagrożeniami wykrywanymi przez IPS,
 - blokowanymi próbami dostępu i exploitami,
 - c) skonfiguruje tworzenie automatycznych alertów o wykrytych anomaliach sieciowych,
 - d) skonfiguruje retencję logów,
 - e) skonfiguruje generowanie raportów i powiadomień dla administratorów.
- 6) przeprowadzi testy funkcjonalne i obciążeniowe w następującym zakresie:
- a) wykona weryfikację poprawności polityk firewall oraz routingu,
 - b) przeprowadzi testy redundancji HA – wymuszone przełączenie aktywnego urządzenia,
 - c) zasymuluje próby włamań, ataków DDoS i innych zagrożeń,
 - d) przetestuje dostęp do zasobów przez użytkowników VPN,
 - e) przeprowadzi monitoring wydajności urządzenia pod obciążeniem,
- 7) opracuje oraz przekaże podczas odbioru przedmiotu umowy dokumentację powdrożeniową zawierającą:
- c) szczegółowy opis konfiguracji zapór,
 - d) procedury przywracania systemu i odzyskiwania danych.
6. W ramach wdrożenia systemu centralnego logowania i analizy zdarzeń Wykonawca wykona poniższe czynności:
- 1) w zakresie instalacji i konfiguracji systemu:
 - a) przeprowadzi instalację tak aby wdrożony system logowania był integralną częścią dostarczonej zapory sieciowej,
 - b) zainstaluje system centralnego logowania w środowisku wirtualnym lub fizycznym zgodnie z wymaganiami zamawiającego,
 - c) zweryfikuje zgodności z dostępnymi hypervisorami (VMware ESX/ESXi, Microsoft Hyper-V),
 - d) przeprowadzi przygotowanie minimalnych zasobów systemowych, w tym interfejsy sieciowe i przestrzeń dyskową,
 - e) skonfiguruje ustawienia systemu, w tym integracji z siecią zamawiającego,
 - 2) w zakresie konfiguracji zbierania i przechowywania logów:
 - a) zdefiniuje polityki zbierania logów z zapory sieciowej oraz innych urządzeń sieciowych, serwerów, systemów operacyjnych i aplikacji,
 - b) przeprowadzi konfigurację komunikacji między systemami zabezpieczeń a centralnym systemem logowania przy użyciu protokołów UDP/514 oraz TCP/514,
 - c) wdroży mechanizmu długoterminowego przechowywania na zasobach sieciowych (SFTP, CIFS, NFS),
 - d) zweryfikuje poprawność zbierania logów i filtrowanie nieistotnych danych,
 - 3) przeprowadzi konfigurację analizy logów i korelacji zdarzeń w ramach której:
 - a) zdefiniuje reguły korelacji zdarzeń dla:
 - malware,
 - aplikacji sieciowych,
 - wiadomości e-mail,
 - systemu zapobiegania włamaniom (IPS),
 - ruchu sieciowego (Traffic),
 - utraconych połączeń VPN i awarii sieciowych,
 - b) skonfiguruje mechanizm alertowania w przypadku wykrycia zagrożeń (powiadomienia e-mail, SNMP),
 - c) przeprowadzi testy skuteczności korelacji i monitorowania incydentów,
 - 4) w zakresie raportowania i monitoringu:
 - a) dokona konfiguracji predefiniowanych raportów, obejmujących:
 - najczęściej wykrywanych ataków,
 - aktywność użytkowników,
 - używanych aplikacji,
 - odwiedzanych strony WWW,

- statystyki połączeń VPN i polityk firewall,
 - b) skonfiguruje możliwość generowania raportów na żądanie lub cyklicznie w formatach PDF i CSV,
 - c) przeprowadzi testy automatycznego przesyłania raportów na wskazane adresy e-mail,
- 5) w zakresie zarządzania i uwierzytelniania administratorów:
- a) dokona konfiguracji dostępu administracyjnego przez protokoły HTTPS i SSH,
 - b) dokona integracji z systemami uwierzytelniania (LDAP, Radius, PKI),
 - c) zdefiniuje co najmniej 4 administratorów z możliwością zarządzania uprawnieniami
 - d) skonfiguruje polityki dostępu do poszczególnych logów i raportów,
- 6) Wykonawca w zakresie testów funkcjonalnych i obciążeniowych:
- a) wykona testy poprawności zbierania i analizy logów,
 - b) przeprowadzi symulację incydentów i testowanie skuteczności wykrywania zagrożeń,
 - c) dokona weryfikacji poprawności integracji z urządzeniami i systemami monitorowania,
 - d) przeprowadzi testy wydajnościowe i optymalizacja zasobów systemowych,
- 7) Wykonawca opracuje oraz przekaże podczas odbioru przedmiotu umowy dokumentację powdrożeniową z zakresu:
- a) szczegółowego opisu konfiguracji systemu logowania,
 - b) instrukcji zarządzania politykami logowania i analizy zdarzeń,
 - c) procedury odzyskiwania i przywracania systemu po awarii,
 - d) dokumentacji integracji z innymi systemami monitorowania.
7. Szkolenie w zakresie obsługi wdrożonych urządzeń i oprogramowania przeprowadzone zostanie w siedzibie zamawiającego, w języku polskim, i obejmować będzie zagadnienia teoretyczne oraz warsztaty praktyczne.
- 1) Zagadnienia teoretyczne obejmować będą:
- a) podstawy działania zapory sieciowej,
 - b) omówienie architektury wdrożonego systemu w tym systemu logowania,
 - c) omówienie podstawowych zasad analizy logów i korelacji zdarzeń,
 - d) funkcjonalność systemu analizy logów,
 - e) przedstawienie integracji systemu logowania z innymi platformami monitoringu,
 - f) obsługę interfejsu zarządzania,
 - g) tworzenie polityk dostępu i zabezpieczeń,
 - h) analiza logów, incydentów i tworzenie reguł korelacyjnych,
 - i) tworzenie raportów i alertów.
- 2) W ramach warsztatów praktycznych wykonawca przeprowadzi scenariusze awaryjne i procedurę odzyskiwania systemu obejmujące:
- a) reakcje na ataki i incydenty,
 - b) odzyskiwanie konfiguracji i testy HA.
- 3) Po zakończonym szkoleniu wykonawca przekaże materiały dla uczestników na które składać się będą:
- a) Podręcznik administratora.
 - b) Instrukcje szybkiej reakcji na incydenty.
 - c) Lista komend i skrótów do zarządzania systemem.
 - d) Certyfikaty potwierdzające udział w szkoleniu.
8. Przedmiot umowy podlegał będzie odbiorowi. Z czynności odbioru zostanie spisany protokół odbioru z udziałem przedstawicieli Zamawiającego i Wykonawcy.

OSOBY DO KONTAKTU W SPRAWIE REALIZACJI UMOWY

§3

1. Strony umowy wskazują następujące osoby, które będą odpowiedzialne za realizację umowy:
- 1) ze strony Zamawiającego:
 - 2) ze strony Wykonawcy:
(imię nazwisko; adres e-mail; nr telefonu)
2. Każda ze stron ma prawo zmienić osoby, o których mowa w ust. 1, niezwłocznie powiadamiając o tym drugą stronę na piśmie lub za pomocą poczty elektronicznej. Zmiana taka nie wymaga sporządzania aneksu do umowy.

WYNAGRODZENIE I ZASADY ROZLICZANIA

§4

1. Strony ustalają wynagrodzenie brutto za wykonanie przedmiotu umowy, zgodnie z ofertą Wykonawcy, na kwotę brutto: zł (słownie złotych:), w tym:
wynagrodzenie netto: zł
kwota podatku VAT: zł.
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszystkie koszty związane z właściwym i terminowym wykonaniem przedmiotu umowy.

§5

1. Rozliczenie za wykonanie przedmiotu umowy nastąpi jedną fakturą.
2. Podstawę do wystawienia faktury stanowił będzie protokół odbioru podpisany przez przedstawiciela Zamawiającego i Wykonawcy.
3. Należność za wykonie przedmiotu umowy płatna będzie przelewem, w terminie do 30 dni od daty doręczenia Zamawiającemu faktury.
4. Wystawiana przez Wykonawcę faktura ma wskazywać:

jako nabywcę:	jako odbiorcę lub płatnika:
Powiat Rzeszowski 35-959 Rzeszów, ul. Grunwaldzka 15 NIP: 813-29-19-572	Starostwo Powiatowe w Rzeszowie 35-959 Rzeszów, ul. Grunwaldzka 15

5. Zamawiający nie udziela zaliczek.

KARY UMOWNE

§6

1. Wykonawca zapłaci Zamawiającemu kary umowne w następujących przypadkach i wysokościach:
 - 1) za zwłokę w wykonaniu przedmiotu umowy - w wysokości 1 % wynagrodzenia brutto określonego w § 4 ust. 1, za każdy dzień zwłoki,
 - 2) za zwłokę w wykonaniu naprawy gwarancyjnej w wysokości 0,05 % wynagrodzenia brutto określonego w § 4 ust. 1, za każdy dzień zwłoki liczonej od dnia wyznaczonego na usunięcie awarii,
 - 3) za odstąpienie od umowy z przyczyn leżących po stronie Wykonawcy - w wysokości 10 % wynagrodzenia brutto określonego w § 4 ust. 1.
2. łączna maksymalna wysokość kar umownych nie może przekroczyć 15 % wynagrodzenia brutto określonego w § 4 ust. 1.
3. Zamawiającemu przysługuje prawo dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych.
4. Zamawiający może dokonać potrącenia wymagalnych kar umownych z wynagrodzenia Wykonawcy.

ODSTĄPIENIE OD UMOWY

§7

1. Zamawiający, oprócz przyczyn wskazanych w kodeksie cywilnym, może odstąpić od umowy gdy:
 - 1) ujawnione zostaną okoliczności świadczące o tym, że Wykonawca złożył w postępowaniu prowadzonym w celu udzielenia zamówienia nieprawdziwe dokumenty, pełnomocnictwa lub oświadczenia,
 - 2) w stosunku do wykonawcy zostało wszczęte postępowanie upadłościowe, o ile będzie miało to wpływ na realizację Umowy,
 - 3) Wykonawca nie będzie wywiązywał się z postanowień niniejszej umowy, w tym zwłaszcza w przypadku zwłoki w terminie dostawy przedmiotu umowy, określonego w § 2 ust. 1.
2. Odstąpienie od umowy następuje poprzez złożenie przez Zamawiającego oświadczenia o odstąpieniu od umowy, w formie pisemnej, wraz z uzasadnieniem przyczyn odstąpienia. Oświadczenie to może zostać złożone w terminie 30 dni od dnia powzięcia wiadomości o wystąpieniu przesłanek wymienionych w ust. 1.
3. Odstąpienie od umowy nie ogranicza Zamawiającemu możliwości dochodzenia kar umownych oraz prawa żądania odszkodowania za niewykonanie lub nienależyte wykonanie przedmiotu umowy.

GWARANCJA I WSPARCIE TECHNICZNE

§8

1. Wykonawca oświadcza, że dostarczone urządzenia objęte są gwarancją na okres 60 miesięcy, począwszy od dnia odbioru przedmiotu umowy.
2. W okresie gwarancji Wykonawca zobowiązuje się zapewnić bezpłatne naprawy dostarczonych urządzeń lub ich bezpłatne wymiany na wolne od wad.
3. W przypadku wystąpienia awarii urządzenia Wykonawca zobowiązuje się do zapewnienia naprawy zgodnie z następującymi zasadami:
 - 1) Naprawa urządzenia rozpoczęta zostanie w następnym dniu roboczym po otrzymaniu zgłoszenia awarii a czas naprawy nie powinien przekroczyć jednego dnia roboczego. Naprawa gwarancyjna dokonywana będzie w miejscu użytkowania urządzenia w godzinach 7:30-18:00. W przypadku zgłoszenia awarii po godz. 15:30 lub w dniu ustawowo wolnym od pracy, jako datę zgłoszenia przyjmuje się datę pierwszego dnia roboczego po dniu, w którym dokonano zgłoszenia.
 - 2) W przypadku gdy dokonanie naprawy nie będzie możliwe w miejscu użytkowania lub czas naprawy przekroczy jeden dzień roboczy, wykonawca zobowiązany jest dostarczyć oraz zainstalować, skonfigurować i uruchomić urządzenie zastępcze o parametrach nie gorszych od urządzenia uszkodzonego.
 - 3) W przypadku gdy naprawa urządzenia wykonywana będzie poza miejscem użytkowania, wykonawca transportuje uszkodzone urządzenie do serwisu, a po naprawie do miejsca użytkowania, na własny koszt i ryzyko a także dokonuje ponownej jego instalacji u Zamawiającego, po czym nastąpi sprawdzenie poprawności działania naprawionego urządzenia.
 - 4) Na czas naprawy urządzenia poza miejscem użytkowania, niezależnie od rodzaju awarii, dysk twardy lub inny nośnik danych pozostaje u Zamawiającego. Jeżeli awarii ulegnie sam dysk twardy lub inny nośnik danych, pozostaje on u Zamawiającego i nie będzie oddawany do serwisu w celu naprawy, lecz zostanie wymieniony na nowy.
 - 5) W przypadku trzykrotnej awarii tego samego urządzenia Wykonawca dokona wymiany urządzenia na nowe wolne od wad.
4. W okresie gwarancji wykonawca zobowiązuje się zapewnić bezpłatne wsparcie techniczne przy rozwiązywaniu wszelkich problemów związanych z działaniem dostarczonych urządzeń oraz systemu centralnego logowania, raportowania i korelacji.
5. W okresie gwarancji wsparcie techniczne świadczone będzie w języku polskim, przez odpowiednio wyszkolony personel inżynierski, telefonicznie lub za pomocą środków komunikacji elektronicznej, w dni robocze w godzinach 7:30-18:00.
6. Wykonawca w okresie gwarancji zapewni bezpłatny dostęp do najnowszych wersji oprogramowania, bez konieczności wykupywania dodatkowych pakietów serwisowych.
7. Korzystanie przez Zamawiającego z uprawnień wynikających z gwarancji nie zwalnia Wykonawcy od odpowiedzialności z tytułu wad lub nienależytej jakości produktów zgodnie z przepisami o rękojmi za wady fizyczne rzeczy.

ZMIANY UMOWY

§9

1. Poza zmianami umowy dopuszczonymi na podstawie art. 455 ustawy pzp, dopuszcza się możliwość zmian postanowień zawartej umowy, w następujących przypadkach:
 - 1) gdy zmiana dotyczy urządzenia wymienionego w „Wykazie rzeczowo-finansowym” w przypadku wycofania go z produkcji i wprowadzeniu zamiennika o tych samych lub lepszych właściwościach. Warunkiem zmiany umowy w oparciu o wyżej wspomnianą okoliczność, jest konieczność przekazania Zamawiającemu oświadczenia producenta o wycofaniu z produkcji danego urządzenia wraz z oświadczeniem Wykonawcy o nazwie proponowanego zamiennika. Wykonawca musi załączyć także karty charakterystyki proponowanego zamiennika wraz z jego ceną jednostkową brutto, która nie może być wyższa niż cena jednostkowa brutto urządzenia wycofanego z produkcji.
 - 2) gdy zmiana dotyczy przedłużenia terminu wykonania przedmiotu umowy jeżeli:
 - a) wystąpią okoliczności, których strony nie były w stanie przewidzieć, pomimo zachowania należytej staranności, mające bezpośredni wpływ na termin realizacji przedmiotu umowy,

- b) konieczność zmiany spowodowana jest okolicznościami pozostającymi poza kontrolą stron, dotyczy to w szczególności takich okoliczności jak zagrożenie epidemiologiczne, zamieszki, akty terroru, zamknięcie granic, rządowe ograniczenia międzynarodowego transportu, utrudnienia na lotniskach i granicach, tj.: okoliczności o charakterze tzw. siły wyższej. W czasie trwania siły wyższej Wykonawca odpowiada za wykonanie umowy na zasadach ogólnych kodeksu cywilnego. Wykonawca dołoży wszelkich starań, aby pomimo istnienia siły wyższej zapewnić ciągłość dostaw oraz zobowiązuje się informować Zamawiającego niezwłocznie i na bieżąco o wszelkich trudnościach związanych z dostarczeniem zamówionych przez niego urządzeń, o których mowa w §1.
2. Termin wykonania umowy może zostać przedłużony o okres, nie dłuższy niż, okres występowania okoliczności, o których mowa w ust. 1 pkt 2.
3. Wszelkie zmiany umowy możliwe będą wyłącznie gdy zostaną spełnione łącznie następujące warunki:
- 1) wystąpienie okoliczności, o których mowa w ust. 1 zostało udokumentowane przez Wykonawcę,
 - 2) Zamawiający uzna i zaakceptuje w formie pisemnej pod rygorem nieważności, że wystąpiły okoliczności opisane w ust. 1 oraz w przypadku, o którym mowa w ust. 1 pkt 2, że wpłynęły one na termin wykonania przedmiotu umowy.
4. Zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności, chyba że umowa stanowi inaczej.

POSTANOWIENIA DODATKOWE

§10

Strony zgodnie postanawiają, że Wykonawca i Podwykonawca nie mogą bez uprzedniej zgody Zamawiającego podejmować żadnych czynności w szczególności zawierać umów, zwłaszcza cesji i poręczenia, których skutkiem mogłoby być przejście na osobę trzecią, na podstawie umowy lub z mocy prawa wierzytelności przysługującej Wykonawcy i Podwykonawcy w stosunku do Zamawiającego, albo wstąpienie osoby trzeciej w prawa zaspokojonego wierzyciela. Wykonawca oświadcza, że zastrzeżenie to zostanie wprowadzone do umowy zawartej pomiędzy Wykonawcą a Podwykonawcą.

§11

Na podstawie art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L z 2016 r. Nr 119, str. 1), dalej „RODO”, informuję, że:

- 1) Administratorem Pani/Pana danych osobowych jest Starostwo Powiatowe w Rzeszowie, ul. Grunwaldzka, 15, 35 – 959 Rzeszów, które realizuje zadania Starosty Rzeszowskiego oraz Zarządu Powiatu. Kontakt telefoniczny: 17 23 00 651, kontakt e-mail: starostwo@powiat.rzeszowski.pl.
- 2) W zakresie dotyczącym ochrony danych osobowych może Pani/Pan kontaktować się pisemnie z Inspektorem Ochrony Danych pod adresem: ul. Grunwaldzka 15, 35 – 959 Rzeszów, lub za pomocą adresu e-mail: rodo@powiat.rzeszowski.pl.
- 3) Pani/Pana dane osobowe przetwarzane będą w celu:
 - a) zawarcia i wykonywania umowy zawartej z Administratorem (art. 6 ust. 1 lit. b RODO) oraz dokonania niezbędnych rozliczeń w związku z jej zawarciem – przez czas niezbędny do realizacji umowy, a po jej zakończeniu dane osobowe będą przetwarzane przez czas potrzebny na wykazanie prawidłowości wykonania wynikających z niej obowiązków do upływu terminów wskazanych w przepisach o archiwizacji;
 - b) wykonywania ustawowych obowiązków Administratora, w szczególności podatkowych i sprawozdawczych (art. 6 ust. 1 lit. c RODO) – przez czas niezbędny do realizacji ustawowych obowiązków Administratora;
- 4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy pzp, a także użytkownicy dostarczonych urządzeń;
- 5) Pani/Pana dane osobowe będą przechowywane przez okres określony zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Z 2011 r. Nr 14 poz. 67 ze zm.) lub w przypadku dofinansowania zadania ze środków zewnętrznych zgodnie z wytycznymi konkursu oraz umowy o dofinansowanie;

- 6) obowiązek podania Pani/Pana danych osobowych jest warunkiem koniecznym do zawarcia i realizacji umowy;
- 7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- 8) posiada Pani/Pan:
 - a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą pzp oraz nie może naruszać integralności protokołu oraz jego załączników);
 - c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
 - d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- 9) nie przysługuje Pani/Panu:
 - a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. b RODO.

§12

1. Wykonawca zobowiązany jest wypełnić obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO, wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał lub pozyska w celu zawarcia i realizacji umowy.
2. Wykonawca zobowiązany jest zastosować środki zabezpieczenia określone w art. 32 RODO w stosunku do danych osobowych pozyskanych w związku z realizacją niniejszej umowy.
3. Wykonawca jest odpowiedzialny na zasadach ogólnych przepisów RODO, za szkody wyrządzone Zamawiającemu, osobie fizycznej, której dane osobowe zostały mu udostępnione lub innym osobom trzecim, w związku z nienależytym przetwarzaniem, bądź zabezpieczeniem tych danych.

§13

1. Wykonawca zobowiązany jest do informowania Zamawiającego o zmianie formy prawnej prowadzonej działalności, o wszczęciu postępowania upadłościowego oraz zmianie sytuacji ekonomicznej mogącej mieć wpływ na realizację umowy oraz o zmianie siedziby firmy, pod rygorem skutków prawnych wynikających z zaniechania, w tym do uznania za doręczoną korespondencję skierowaną na ostatni adres podany przez Wykonawcę.
2. Wszelkie spory mogące wyniknąć na tle realizacji postanowień niniejszej umowy strony poddają rozstrzygnięciu sądu właściwego miejscowo dla Zamawiającego.
3. W sprawach nieuregulowanych niniejszą umową, mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2024 r. poz.1061 ze zm.), ustawy pzp oraz postanowienia SWZ.
4. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, z przeznaczeniem dwóch egzemplarzy dla Zamawiającego oraz jednego egzemplarza dla Wykonawcy (*w przypadku zawarcia umowy w formie elektronicznej ust.4 zostanie usunięty*).

Zamawiający:

Wykonawca:

Kontrasygnata Skarbnika

Załącznik:

Wykaz rzeczowo-finansowy

Lp.	Określenie urządzenia/oprogramowania	Ilość	Stawka podatku VAT (%)	Wartość brutto (zł)
1	SPRZĘTOWA ZAPORA SIECIOWA PRODUCENT, NAZWA : Numer produktu lub kod producenta: Z urządzeniami zostaną dostarczone licencje: <i>(rodzaj licencji zostanie określony zgodnie z ofertą wykonawcy)</i>	2 szt.	23	
2	SYSTEM CENTRALNEGO LOGOWANIA I ANALIZY ZDARZEŃ PRODUCENT, NAZWA : Numer produktu lub kod producenta: LICENCJA: bezterminowa z bezpłatnym wsparciem technicznym na okres: 60 miesięcy.	1 szt.	23	
RAZEM WARTOŚĆ BRUTTO				

Zamawiający:

Wykonawca: